Plots of Intelligence Surveillance
Dramas of Institutional Identification

Gianluca Miscione
School of Business
University College Dublin

European Group on Organization Studies (EGOS) conference
July 3rd – 5th, 2014
Rotterdam, The Netherlands

Abstract. Recent revelations of intelligence surveillance are an unprecedented breakdown of contemporary communication functioning, therefore offer novel insights about how it has worked normally. The contrastive description of the Wikileaks and Snowden's events show unexpected paths to address responsibility and enact performativity globally. In both cases, hundreds of thousands of highly sensitive documents make their management significant in terms of how practices unfold on and beyond information infrastructures. The two cases engender two approaches to information management, one more closely derived from the original culture of the internet, the other sensitive to more broadly accepted social models. In this context, unearthing the usually invisible role that information infrastructures play in contemporary social praxes helps in recognizing how narratives can play a role in understanding online information and related action-nets, therefore broader social and political implications.

Keywords: intelligence, surveillance, information infrastructures, Snowden, Wikileaks, narratives, realism.

"Among all the things of this world, information is the hardest to guard, since it can be stolen without removing it"
Erving Goffman

"It is dangerous to be right when the government is wrong."
Voltaire

"All human beings have three lives: public, private, and secret"
Gabriel García Márquez

In the last week of October 2013, it was revealed that political and personal communications of the German Chancellor were spied upon by US secret services. Puzzlement rose as no one seemed to know whom to hold responsible. US National Security Agency (NSA), which operated it? US Congress, that voted the Patriot Act, which allows those activities? President Obama, who did not stop spying on allies? Al Qaeda, whose actions sparked global outrage and so created the conditions to allow an inescapable, globally spread intelligence activity? Initial Internet protocol designers, who came from the open culture of the sixties and seventies and did not bother to implement identification technologies, so facilitating large scale anonymous online activities decades later? Or the German counter espionage and the organization that implemented the security system of Merkel's phone? Or even the global community of mathematicians, who claimed the infallibility of their prime numbers theorems, so making everyone else overlooking the dangers of translating theorems into security algorithms and software?

Which organizations should perform a reaction? Merkel herself, with her memories of Stasi, confronting her ally face to face? The national diplomacies? The EU, which is supposed to have a single face to the outer societies? Engineers, who should not have assumed the scientific primacy of beautiful simplicity of math over the messy world of technology in practice? Telecommunication companies, made responsible of enacting appropriate security and privacy measures?

In recent years the USA has repeatedly accused other countries, China in particular, of spying and hacking its computer systems. Being the center of the internet infrastructure was said to expose the USA more than less connected countries. The

revelations about the National Security Agency (NSA) suddenly showed how this architectural centrality was turned inside-out to US advantage into a sort of global panopticon. We have come a long way since when, in 1929, US Secretary of State Henry Stimson banned the decryption of diplomatic cables because “Gentlemen do not read each other’s mail”.

Attributing responsibility is a central aspect of organizing. Following actual processes of responsibility attribution can tell us about the inner workings of organizing, especially in contexts where activities are loosely informed to organizational structures, formal procedures and consistent jurisdiction.

As there is no worldwide government, international relations have always been characterized by the anarchy of nations, i.e. the absence of a universal sovereign, of a worldwide consistent legal system and of a hierarchically superior above nations whose power can enforce laws and resolve disputes. Against this broad background, there is not much novelty in what signals intelligence has been doing since at least the Enigma code[1] was broken: trying to detect what allies and enemies were about to do. What has become more prominent in the increasingly multipolar and interdepended world today is the way intelligence surveillance interplays with privacy and international public opinions by sharing the same basic information infrastructures.

Privacy, intelligence agencies, public option might have seemed far-fetched, but recent history proves the opposite. Indeed, large scale information technologies, which exceed any individual state and single jurisdiction, expose daily their designers and users to globally disperse and patchily regulated interactions and social relations. International relations are not an exclusive concern of governments and multinationals anymore, but of any contemporary organization and even individuals. So, the possibility of being snooped upon grew together with the outreach of our digital communications.

Surveillance has two equally relevant sides: large organizations, governments in particular, always pushed to watch ‘their’ people. Citizens periodically manifest intentions to exact accountability by watching the watchers (for example (Miscione,

[1] The Enigma code refers to the encryption code used by the Nazi Army to hide communications for their operations. The efforts to decrypt it allegedly allowed the Allies to win the Second World War, and certainly originated fundamental knowledge for computer science and contemporary informatics.

2011; Verplanke et al., 2010). Respectively, the effect of open networks on this situation is twofold: government agencies like the NSA say that surveillance is the price for keeping the internet open, which means: having realized how difficult to regulate the internet is, Western governments opt for letting it go and surveiling. Citizens and multinationals whose business depends on cloud computing do not seem to agree on this arrangement. On the other side, it should not be overlooked that states have never had so many troubles in keeping their secrets. So, asymmetry of information is being eroded on both sides.

In an age of dispersed organizing processes and huge unstructured data 'oceans' allowed by open information infrastructures, two cases of whistleblowing from recent news help illustrate a wide and powerful call to responsibility far beyond what a narrow focus on bounded organizations could explain. Indeed, the current breakthrough in transparency and accountability is being led by motivated, highly technically skilled players who pulled together people and technologies in unexpected ways.[2] The two cases considered here are usually referred to as Wikileaks and Snowden (it will be made clear that the most visible actors are not necessarily the key ones). In both cases, hundreds of thousands of highly sensitive documents had to be managed under the most extreme conditions: travelling and hiding while 'tailed' by the mightiest intelligence agencies and diverse national governments, with relatively scarce resource at disposal, exposed to lack of reliable jurisdiction (and of course no peer reviewed literature to rely upon). Those conditions make the management of these data significant in terms of how practices unfold on and beyond contemporary information infrastructures. The two cases engender two approaches to information management, one more closely derived from the original culture of the internet, the other sensitive to more broadly accepted social models. The contrastive analysis of two cases shows first how organizing exceeds organizations, and the role of emplotting and sense-making that established institutions

[2] As humor reflects the sense of time, two ironic quotes can be significant here: "The pen is mightier than the sword, and considerably easier to write with" said Marty Feldman (active till the seventies). In the latest 007 film (Skyfall 2012), a young Q puts James Bond – who says that youth is no guarantee of innovation – firmly in his place: "I'll hazard I can do more damage on my laptop sitting in my pajamas before my first cup of Earl Grey than you can do in a year in the field". The former does not apply to these cases, which instead show how difficult is to use contemporary writing technologies to contrast established patterns of communication. The latter quote hints at a rebalancing of organizational power where the technologists are not simply providing fancy tools (like explosive cigars).

like press and free speech continue to play, although in novel ways. Here I follow an interest in surfacing the role of infrastructures, as in Pinch (2009) also engaging with the actual workings of technology (Pinch, 2008). I rely on the Neoinstitutional difference between institutions intended as social models, and organizations as actors (North, 1990; Powell & DiMaggio, 1991)

The rest of the article is organized as follows: after a theoretical framework that spans organization and communication studies, the research methodology is described. Two case studies are described at the level of detail needed for a comparison. Finally, the possible theoretical relevance is discussed and conclusions drawn.

Mass media to mass data, whose narratives?

Even though they tend to be studied by diverse disciplines, it is commonly accepted that writing technologies, organizational forms and public opinion have been interwoven since at least the invention and massive deployment of the printing press (Goody, 1986; McLuhan, 1962; Ong, 1982). Acknowledging both the centrality of communication in contemporary societies and the impossibility of identifying universal truths, Habermas (1989) put forward the proposal of the “ideal speech situation”: an open agora where any issue can be brought in and rationally discussed with the objective of democratically govern societies. According to this view, social institutions such as the mass media have to play a paramount role not only in informing citizens but also in enabling them in participating to debates of public significance. However, the media evolved into large conglomerates governed by specific and not rarely particularistic interests, which turned to be a concern for a democratic public sphere.

A perfect epitaph for independent journalism comes from an ex-editor of the UK newspaper The Independent who disagreed on The Guardian publishing documents leaked by Snowden: “If MI5 warns that this is not in the public interest who am I to disbelieve them?” This self-confinement of part of journalism may call to mind an aspect of the debate between Habermas and Luhmann, the latter claiming that organizations are governed by auto-poesies. Therefore media organizations – as any other –

reproduce themselves rather than serving society as envisioned by the former's normative theorization.

The circularity of news production is central in Czarniawska (2012) organizational study of three different news agencies. The actor-network theory's principle of symmetry (Latour, 2005), i.e. accounting for both humans and artefacts in equal terms, allowed Czarniawska to account for the variety of technologies and organizational arrangements at work together. Different cases and diverse situations concur in showing the circularity of news production. The circuits she identified may shake the belief of those convinced that news objectively report the reality out there; underneath, the influence of Luhmann on this analysis can be recognized. The news that Bloomberg reporters could have extra access to Bloomberg terminal users' information[3] adds a 'cyberspace flavor' to the same kind circularity: indeed for Bloomberg, providing information management tools was a way to enhance the outreach of its own sight in news production. Not differently in principle, but on a widely larger scale, the centrality of the USA in the internet architecture provided it with unparalleled access to world wide data flows.

So, if the open and rational public sphere envisioned by Habermas seems to remain utopic, other forms of breaking media circularity can be considered. The fourth estate, not least celebrated by Welles in "Citizen Kane", has a long lasting tradition. It became legitimized in the nineteenth century (Conboy, 2004) and always relied on non-journalist informants. Whistle-blowers have often found support and resonance on the press, even more than on other media. Still, through the last decades, mass media have been criticized for being complacent to the powers they were supposed to watchdog.[4] The alleged departure of mainstream media from investigative journalism has created a void that contemporary discontent public opinion proved eager to see filled.

Initial enthusiasm for the so called blogosphere found ground in the resentment against established media organizations. We were a few years before the turn of the millennium when the internet seemed to promise openness and democratization to every niche of societies, for instance Poster (1997) and Kerckhove (1997). Beside

[3] http://www.businessinsider.com/bloomberg-news-goldman-2013-5 (last accessed on November 26th, 2013)
[4] For instance the non-governmental organizations Reporters Without Borders publishes yearly the World Press Freedom Index.

widely used blog platforms, Indymedia is seen as an early attempt in this sense (Anderson, 2010; Hintz, 2013).

Following such enthusiasm, open participation rather than professional journalism would have counterbalanced dominant interests by watchdogging the powerful, showing their responsibilities and exacting accountability. Since then, 'citizen journalism' – and lay people's data production in general, usually called web 2.0 – has certainly been challenging journalism (Boczkowski & Mitchelstein, 2013; Bruns, 2012; Conboy, 2004; Landert, 2014; Lewis, 2012; Newman, Dutton, & Blank, 2012; Ostertag & Tuchman, 2012). Nowadays indeed, many journalists act more like opinion leaders and tend to moderate and edit content produced online by 'crowds'; by the time photoreporters have flown to war or disaster sites, plenty of pictures are already made publicly available by locals; the mode of communication is becoming more personalized also because of comments on online news and journalists eliciting materials from readers/eyewitnesses; readers do not seem willing to pay for information that can be found elsewhere for free, and so on and so forth. Benkler (2006) identified the possibilities afforded through technological advances such as the advent of the internet in what he termed the networked public sphere. Dutton (2009) claimed that internet-based communication allows the emergence of a 'fifth estate' distinct from the fourth.

Within this broad context, close-to-technology whistle-blowers have been breaking some of those circularities, so challenging the established balance between stage and backstage for both watchers and the watched. Benkler (2012) study of the events surrounding the Wikileaks document released in 2010 provides a rich set of insights about the weaknesses and sources of resilience of the emerging networked fourth estate. Later, he (Benkler, 2013) writes "it marks the emergence of a new model of watchdog function, one that is neither purely networked nor purely traditional, but is rather a mutualistic interaction between the two."

So, if an utopically democratic public sphere remains chimerical and investigative journalism has always been part of the fourth estate, what new can we learn from the recent wave of whistle-blowing? As anticipated, the argument here focuses on the

organizational significance of the way privacy, intelligence and infrastructures intersect, thus how organizing takes place.

Shyness of organization studies to see beyond formal organizations may leave contemporary issues to groundless analyses. Inadequate conceptualizations may show their limits starkly when empirical occurrences shed light on their blind spots. Although it is needless to say that the views on recent leak cases are diverse, it stands clear that focusing on individual organizations that are assumed to have boundaries and to perform according to their functions, is empirically of little help, theoretically questionable (Czarniawska, 2008; Czarniawska, 2013a) and ethically inadequate (Floridi, 2012). Knorr-Cetina, Schatzki, and Von Savigny (2000), Czarniawska (2008) and Nicolini (2012) among others have departed from reified views on organizations and focus on the way organizing processes unfold. Considering organizations as an outcome of organizing processes rather than a pre-requisite provides the best position to capture and explain the information infrastructure-related cases addressed here. So, relevant notions from information studies are introduced.

As it is hard to find any online data that is not part of a database in a way or another, “it is vital to dissolve the current disjunct between database (as technical storage medium) and policy (as way of acting in the world). The production of the database is productive of the new world we are creating” (Bowker, 2000). Manovich (1999) spotted that databases, compared to other types of information goods like novels or movies, are not dramatized. I interpret his position in the sense that databases have a structure, based on a consistent classification system, but do not have a pre-defined order of parts that leads towards a message. If emplotted information goods are like walkpaths, databases are more like buildings or games: they do not inscribe a single preferential line of fruition. Rather, inscriptions and affordances facilitate some paths and conceal others. Databases have no plot, intended as a single meaningful way of connecting their elements. If information in databases trades plot for open-endedness, online data go one step further by giving up consistent structure as well. In this sense Berners-Lee (1989) original proposal for the World Wide Web overtook consistent classification

systems of more traditional databases, so limiting the domain of relevance of information infrastructures a-la' Bowker and Star (1999).

Opening the dams of data structure and access has flooded most of us with information overload for quite some time now. Still, our sense-making capacity did not collapse completely as in Weick (1993) disaster analysis. Possibly, an escape fire (or a raft to stay with the water metaphor) are narratives. Indeed, information keeps making sense to people to the extent it resonates with recognizable narratives. Reformulating Richardson who wrote that "firms are islands of planned coordination in the sea of market relations" (Powell, 1990), one could say that narratives are sailing routes in data oceans. Or better, paraphrasing Walter Benjamin's "ideas are to objects as constellations are to stars": narratives are to data as constellations are to stars. In less evocative terms, narratives are considered here as a meaningful (not necessarily causal) ways of connecting events. "The narrative mode of knowing consists in organizing one's experience around the intentionality of human action. The plot is the basic means by which specific events, otherwise represented as lists or chronicles, are put into one meaningful whole" (Czarniawska, 1999). If experience does not necessarily happen in dramatized forms, narratives are sense-making devices to the extend they create an arch or tension towards a meaningful interpretation or prospect. In Ireland for example, the release of snooped phone calls in which reckless decision makers of main financial organizations which were about to fail, framed the whole understanding of financial data and activities of decades, also in the eyes of other European partners[5].

In sum, communication technologies constitute a public sphere that is not progressively informed by rationality. Media organizations tend not to compensate for unequal distribution of power in societies, so a new wave of investigative journalism leverages information infrastructures managing large datasets of confidential data. To clarify a framework on the fringes of communication studies, I anticipate the message of my story: the effects of Snowden's leaks have been more clearcut because they aligned with the Western established narrative of free speech and investigative journalism.

[5] http://www.irishtimes.com/news/world/europe/conned-a-german-view-of-ireland-1.1454115

Instead, Wikileaks originated more contradictory reactions when it published a huge dataset of hundreds of thousands of unedited diplomatic cables leaving it to anyone to make sense of it in their own way. And we all did it, very diversely.

Research approach

Through the case-studies, the principles of focusing on the actual doings (Nicolini, 2009) rather than on the formal organizational structures, and of following the actors (Latour, 2005) was the starting point. Following Czarniawska (2011) advice that "organization scholars should be studying construction and maintenance of connections among collective actions", this study investigated actions and their repercussions also beyond main actors themselves. This is found to be the most appropriate way to understand recent cases of whistle-blowers who quickly and effectively reached the global public opinion trailblazing unanticipated paths.

The many footprints left on the network by studied activities in their trajectories are crucial empirical data sources. Indeed, documentary studies have an unprecedented methodological potential because of wide availability of data to trace back the actual trajectories of actions, to see how things were perceived at different points in time by the variety of actors involved at different stages. The difference with what was possible before the "web 2.0" is clear comparing these data sources with post-hoc interviews, which have been a major way of reconstructing case-studies. First, an interviewer cannot avoid the past to be reinvented by the interviewees depending on subsequent developments. Second, big datasets facilitate to trace the network of connections far beyond the most visible names that often stories are attached to.

In practice, it is impossible to collect data about actors that could undertake future stealth and often risky actions. Who would have conceived interviewing Julian Assange or Edward Snowden before their clamorous initiatives? There is no escape from the constraints of the present before the future happens. But, if we look at the past as a sequence of presents as they are recorded on online databases of different sorts, each time we can see fragments of how past, present and future were perceived. Then we can compare them to what happened next. Traces of what was present at different points in time are retrievable from the limitless amount of data publicly available. In other

words, big data is mostly exploited here for the unprecedented possibility of identifying retrospectively meaningful angles on data about naturally occurring events of chosen cases. For instance it is possible to see how Assange's past as hacker defined his handling of Wikileaks and how a mission in Geneva undermined Snowden's faith in US intelligence operations.

Empirically, this is basically a documentary study of materials publicly available online. Data collection was concentrated on two periods of time: April through December 2010 and June 2013 through March 2014. However, relevant materials made public in other moments have been considered as well. Contrary to most documentary studies, I did not have to visit any remote library and I do not rely on any exclusive data source. As any reader can easily check online the happenings and revelations referred to here, I will not concentrate on describing the events beyond the details relevant for the study.

A point in space that contains all other points in space and time[6]

The Pandora box opened by contemporary whistle-blowers revealed the intelligence agencies' decade long effort to overcome all obstacles to surveillance, i.e. privacy law, international agreements, encryption technologies, software backdoors, stolen keys up to the active manipulation of standards, which basically means moving upstream to manipulate science.[7]

There is a relevant overarching reason for the NSA case mobilizing so fierce reactions, especially from the more technically sensitive communities from whom all this sparked: revelations showed that the NSA has been able to reach anyone, anywhere, invisibly. So, it falsified a totemic assumption of online cultures: on the internet there is always an elsewhere. In front of the end of their mundane heterotopia, the composite milieu of hackers, geeks, netizens (if such categories mean something) literally freaked out for claustrophobia. In fact, it is worth stressing how their radically open approach to information technology and management derives from entrenched distrust for formal organizations. Indeed, it is believed that if information is free, no organization can

[6] The reference here is to Borges' short story "The Aleph". Anyone watching that point can see everything in the universe from any angle simultaneously and at any point in time.

[7] All released documents can be found on Wikileaks website and here: https://www.freesnowden.is/category/revealed-documents/index.html

consolidate. The totem of limitless space is built on the taboo of appropriating information. Such views are typical of hackers' culture and also manifests in the principles and practices of free and open source software (Coleman & Golub, 2008; Coleman, 2004, 2011; Miscione, 2000). The invisible omnipervasiveness of NSA broke the social pact that ties free information to freedom from organizations. A taboo was infringed, reaction was commensurate.

Both cases described here take their moves from those highly networked social environments, are relatively micro in size (no more than dozens of actors) and globally distributed at the same time. This is typical of contemporary actions exploiting information infrastructures. This rather typical online organizational form – fluid to say the least, globally dispersed, highly decentralized but not necessarily flat – corresponds to the sense that no established organization is too big to challenge because hackers can always find an Achilles' heel to exploit (Miscione, 2000). Indeed, today whistle-blowers leverage an important aspect of contemporary communication: organizations of all sorts as much as individuals are unprecedentedly exposed to unintended use of digital data by or about them.

A here relevant subset of hacking culture is cryptoanarchists, from where most strong privacy tools originated and to whose principles several key actors of those cases refer to. The two cases considered here are commonly referred to as Wikileaks and Snowden. Someone may object that the latter is the evolution of the former. This might be plausible, even though there are fundamental differences that will emerge later. Actually Benkler (2012), which was written before Snowden's case, shows how there was a progressive increase of involvement of the established press. Anyhow, this may suggest that organizational learning and consolidation of actor-networks might have taken place across relevant actants (Corvellec & Czarniawska, 2014).

Wikileaks: all in

Wikileaks was founded in 2006 and describes itself as an "uncensorable system for untraceable mass document leaking"[8]. Wikileaks provides access to anonymous

[8] http://www.theguardian.com/media/2010/jul/14/julian-assange-whistleblower-wikileaks (retrieved on May 15th, 2014)

contributions of raw, unprocessed and unedited data as opposed to filtered, accredited and standardized information provided by established media like news agencies (Boczkowski, 2009; Czarniawska, 2012). Recognizing that power is also based on visibility and invisibility[9], Wikileaks aimed beyond the curtains that separate stage and backstage to reverse visibility of the surveilled and invisibility of the powerful (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012). This has been pursued through a socio-technical alliance of cryptographic technologies and an organization that spans different jurisdictions: it operates so by deploying available cryptographic technology to ensure the anonymity of whistle-blowers and the operational reliability of its infrastructure by mirroring its data on servers under diverse jurisdictions (so to always have a foot in a safe place) and adopting diverse money transfer tools including Bitcoin, a peer-to-peer e-currency. This is part of a tacit deal, because Wikileaks relies on mutuality: its contributors provide information while relying upon the veil of anonymity provided to them. In fact, Bradley Edward Manning[10], the US soldier who collected the diplomatic cables and blew the whistle via Wikileaks in 2010, was identified and arrested after a person he chatted with about his leaks reported him.[11]

Julian Assange, founder of Wikileaks and a long time hacker himself, simply did what any open source software developer does continuously: making unrefined materials publicly available to allow anyone to see what goes on and possibly participate, because "Given enough eyeballs, all bugs are shallow" (Linus Torvalds). Underneath one can spot the belief in the "wisdom of the crowds" (Surowiecki, 2005) and the typical hackers' resentment towards established organizations, consistently perceived as obstacles to organizing. It has also to be underlined that making data public is a way to reduce the mounting pressure on leakers because, once data is public is out of their control.

Besides not having the property rights to publish the information, the difference from open source software is that the general public could read and understand what was publicly released. And it was not indifferent. In fact, public opinion has been polarised

[9] An original angle relying on Ervin Goffman's work is Pinch, T. 2010. The invisible technologies of Goffman's sociology from the merry-go-round to the internet. ***Technology and Culture***, 51(2): 409-424.
[10] He started sex reassignment to become Chelsea Elizabeth Manning.
[11] It is worth noting that a private soldier could access data from all US embassies because those information systems had been mindlessly integrated in the first place, overlooking the risks this trendy choice would entail.

since 2010, when Wikileaks released 251,287 US diplomatic cables[12] and in particular a video of what had been defined a 'collateral murder', but revealed unnecessary violence of US Army in Baghdad. Overall, those cables exposed how governments operated behind closed doors. Website use instructions exemplify quite clearly Wikileaks open-ended approach to information management: "Search for events that you remember that happened for example in your country. You can browse by date or search for an origin near you. Pick out interesting events and tell others about them." It may sound written for Facebook friends, but it is about secret diplomatic documents.

Another example of technologically rooted and highly decentralized organizational arrangement is Assange's 'insurance file': in anticipation of arrest or even assassination, Assange released publicly a large encrypted file allegedly containing all leaked documents, more than those published. The threat was that if he was withheld from releasing materials, the decryption key would be released for anyone to access the file content. In 2012, trying to avoid arrest in the UK for extradition to Sweden for a trail for sexual violence, Assange found refuge in the Ecuadorian embassy in London and was granted asylum. He has been confined in this small foreigner jurisdiction ever since as a self-proclaimed "security reporter refugee".

The large amount of unstructured data released by Wikileaks due to its radical openness, should not be dismissed as confusing and minoritarian, therefore not relevant. The lack of a single straightforward message of appeal to the public opinion beyond absolute transparency for governments, made the Wikileaks case highly unpredictable. Indeed, some of those cables seem to have fuelled the completely unexpected Tunisian revolt of 2010, and then the Arab Spring[13]. More careful analysis of those hundreds of thousands of documents may produce effects on the longer term. No unique narrative may mean many narratives yet to be found.[14]

[12] http://wikileaks.org/cablegate.html (last accessed December 6th, 2013)
[13] This view is mentioned for instance in the BBC Documentary "WikiLeaks: The Secret Life of a Superpower"
[14] Perhaps it is not a chance that Eric Schmidt, former CEO of Google – the main company organizing online data – interviewed Assange for his book "The New Digital Age: Reshaping the Future of People, Nations and Business" (transcript: http://wikileaks.org/Transcript-Meeting-Assange-Schmidt.html)

Snowden: plotting with data

Snowden did not want that his motivations were diluted in a large anonymous dataset. So he chose a dramatic, and in a sense more traditional, way of playing the cat-and-mouse game with authorities. Snowden's role, in this story, corresponds to Manning's not Assange's, but the process he started was quite different. Initially, Snowden was a contractor working as network administrator for the US National Security Agency but took part in higher profile cybersecurity activities like providing Obama with support during the NATO summit in Romania in 2008[15].

While at NSA, "I could watch drones in real time as they surveilled the people they might kill," he told Greenwald, the US journalist of the UK newspaper The Guardian who reported the leaks. "You could watch entire villages and see what everyone was doing. I watched NSA tracking people's Internet activities as they typed. I became aware of just how invasive US surveillance capabilities had become. I realized the true breadth of this system. And almost nobody knew it was happening" as revealed in the recent book by Greenwald (2014). In front of this situation, Snowden made his first contact with Greenwald in December 2012 under the pseudonymous of Cincinnatus, an ancient Roman statesman and farmer who was made dictator to solve a crisis and resigned two weeks later, after resolving it. For months, communications were not successful because the journalist was not adopting the cryptographic technologies the whistle-blower asked him to use. Things started to come together in April 2013. In a move that reminds of the Cold War spy stories, Snowden flew from Hawaii to Hong Kong (China, but tied to the West and its values of freedom) where he met Greenwald and a few trusted journalists.[16] Snowden always intended to reveal his real identity rather than remaining a faceless whistle-blower but journalists insisted he waited after the first releases of top secret materials, otherwise public attention would have focused on him rather than on his revelations. Shortly after the first releases, a few video appearances gave the public an image of him as a rational and trustworthy source, rather than an

[15] More details are reported in NBC interview to Snowden aired on Wed May 28th, 2014.

[16] Face to face, "with a hint of embarrassment," Greenwald recalls, Snowden admitted to have been influenced by videogames in his decision: "The protagonist is often an ordinary person, who finds himself faced with grave injustices from powerful forces and has the choice to flee in fear or to fight for his beliefs. And history also shows that seemingly ordinary people who are sufficiently resolute about justice can triumph over the most formidable adversaries." Greenwald, G. 2014. ***No place to hide - Edward Snowden, the NSA, and the U.S. Surveillance State***: Metropolitan Books.

insane person that certainly NSA would have tried to depict. Later, while transiting through Moscow airport, he got blocked and he is now in Russia on temporary asylum.

Here, I am not listing the unheard-before outreach and scope of NSA surveillance, as it has filled newspapers everywhere for a year now. Among the many leaked documents there were those about the eavesdropping of the German Chancellor's communications, that opened this article. From all those leaks, two aspects of Snowden's approach emerge consistently: he sees his actions as patriotic and he declares himself to be in favour of transparency and public debate about those issues, not against intelligence activities. For instance, in an interview to Vanity Fair, which demonstrates the different audiences Wikileaks and Snowden talk to, he distances himself from hacking radicalism: "On the crucial ways he differs from WikiLeaks founder Julian Assange: 'We don't share identical politics. I am not anti-secrecy. I'm pro-accountability. I've made many statements indicating both the importance of secrecy and spying, and my support for the working-level people at the N.S.A. and other agencies. It's the senior officials you have to watch out for."[17]

The saga of revelations, masterminded by Greenwald, peaked with US President Obama who, under mounting domestic and international pressure, had to respond of US intelligence's activities. The interpretative duel between leakers and US government (UK remained quieter) culminated in mid-January 2014 with Obama's public speech about the NSA and the seemingly out-of-control American surveillance state. It is remarkable to note that the ground for the contrast to gain legitimation with the public opinion was set by the leakers. Indeed, Obama had to open his address claiming that also intelligence is a patriotic activity, as it facilitated US independence from their colonizers, for instance. The rhetorical difficulty was how the first black president could justify state surveillance that for decades impeded Afro-Americans' civil rights movement. Another inescapable dualism was between US constitution, that guaranties citizens vs. the state and security, which became a paramount concern since 9/11. Of these and other dilemmas, Obama could not choose one or the other side, so he basically called for pragmatic and working arrangements. The fact that this speech was a rhetorical

[17] http://www.vanityfair.com/online/daily/2014/04/edward-snowden-interview

exercise rather than a change of policies is confirmed by the little changes that NSA has being undergoing. Still, it was paramount to try to win the duel to reduce risk of others potential whistle-blowers being inspired by those spectacular revelations.

His speech was probably the first presidential speech that can be entirely used in an information management course. He crafted his argument away from Orwellian dystopias and towards the search for convergence at organizational and technological levels. But, the solutions outlined sounded quite Kafkian, as if reducing the grades of separation from suspected terrorists to surveilled people from three to two would solve the issues direly brought to public sight. Still, this kind of protocoled changes reminds that the NSA has grown into a datamining bureaucracy with nearly 100,000 employees and contractors, and 52.6 billions USD annual budget[18]. It is worth paying some attention to how Obama's speech was received by Assange and Snowden. The former saw nothing in Obama's speech[19], which is consistent with his paramount sensitivity for data. Instead, the latter can claim victory because he wanted to bring public opinion's attention onto those issues.

Among the several recent developments, some are particularly remarkable: further revelations contradicted Obama and claimed that NSA conducted also industrial espionage; The Washington Post and The Guardian were awarded the Pulitzer Prize, software developers of all walks of life have been called to develop technologies to embed a higher protection of privacy straight into technology. This was endorsed by Berners-Lee, inventor of the Web, proposing a Magna Carta of the Internet and adding that "we need to encode our values not just in writing but in the structure of the internet"[20], which echoes DeNardis (2012) focus on the levers to govern the internet. Finally, for the time being, in mid-May 2014 it was announced that both 007's producers and Oliver Stone bought the rights for this story from Greenwald.

And now that all that information is dangerously stored in one single place in Maryland, and while public opinion waits for Hollywood to dramatize this story on silver screens, I look forward to seeing what happens with the people who are certainly trying

[18] http://www.washingtonpost.com/world/national-security/black-budget-leaked-by-edward-snowden-describes-nsa-team-that-hacks-foreign-targets/2013/08/30/8b7e684c-119b-11e3-bdf6-e4fc677d94a1_story.html
[19] http://www.youtube.com/watch?v=kIZ0uudhYZg
[20] https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript

to gain access to NSA humongous dataset with any possible means. With literally global interests recorded there, I have no doubt that right now the most skilful hackers on Earth (including those working for intelligence agencies) are picking up the challenge of priding their egos by getting their hands dirty in such unprecedented honeypot of data that not the NSA, but our fears ultimately created.

Playing the flute rather than just blowing the whistle

Whatever happens to those cases, their comparison shows some of the peculiarities of contemporary organizing and may develop their conceptual understandings.

It is important to stress that in terms of organizational functions, Greenwald (not Snowden) corresponds to Assange and The Guardian and other registered newspapers like The Washington Post, which played a major role in the Water Gate, correspond to the platform Wikileaks to voice the whistle-blowers. So, the two actor-networks (whistleblower-mediator-platform) described above are: Manning-Assange-Wikileaks (MAW) and Snowden-Greenwald-Guardian (SGG).

MAW and SGG have certainly been revitalizing the fourth state, but in different ways and with different outcomes. MAW opted for pure transparency the hacker way, therefore no curation of content, which was left to anyone to ‘datamine’ and make sense of. In spite of immediate outrage, it took months to journalists to distil gossips about leaders’ questionable behaviors from relevant geopolitical insights. SGG accorded upfront a more prominent role to traditional investigative journalism to focus, select and publish: so far, of the 50 to 200 thousands documents that Snowden has allegedly acquired, only few hundreds have been made public.

Although the situation is far from stabilized, comparing the consequences to date on the corresponding actants of the two actor-networks can be relevant: Manning underwent trial and received a sentence of 30 years in prison, Snowden is on temporary asylum in Russia and Germany and other countries are considering protecting him. Assange is practically under house arrest in the Ecuadorian Embassy in London whereas Greenwald has been offered 250 million USD to create and manage The Intercept, a watchdog website for investigative journalism. Wikileaks is under continuous pressure while The Guardian and The Washington Post won the Pulitzer Prize.

By playing it more traditionally, by giving space to established media, SGG could leverage a level of legitimation that MAW never gained[21]. Indeed, in public opinion ears, freedom of speech sounds far more appropriate when it is about clear and well-timed stories like those published by newspapers rather than an unstructured dataset full of gossips of dubious public interest. So, Assange (the public face of MAW) had little more than his own persecution to dramatize on the media stage, therefore to offer for international public opinion sense-making. On the other hand, SGG could claim they had an order to restore as their goal: having watchdogs addressing responsibilities of the powerful. From SGG position, it is more convincing to appeal to the First Amendment and whatever guaranties free speech. So that, SGG gets legitimation by the strong plot of Western democracies being based on freedom from governments. Obama indeed had to respond on those grounds whereas, except some heated early reactions, few from the Obama's administration had to respond to Wikileaks at all. Free speech can counter-balance governments' argument of need of secrecy to protect security after 9/11 more than hackers' sub-cultural claims that "information wants to be free". So, MAW and SGG's informational points are pretty similar, but they tie into narratives of quite different resonance, therefore performativity. Also a paradox should be highlighted: Wikileaks' radically open approach relies on the wisdom of the crowds, but when the bigger crowd of general public opinion and major national interests, far broader than internet culture, came into his picture, the situation got out of hands.

The comparison of these trajectories show how rhetorical capacity proved to be determinant. For these reasons, the recognition of the role of media and free speech as institutions made SGG more legitimized, thus more effective in affecting world leaders' agendas.

Media Framing and Political Overflow

The cases presented above confirm how established communication circuits can be hard to question. In this sense, the organizations that rely upon those circuits (media

[21] The two cases discussed here match quite neatly with Don Buchla's vs. Moog's distinct approaches to the music synthesizer. The latter was more successful also because limited the range of possible sounds by adopting the piano type of keyboard, as discussed by Pinch, T. 2008. Technology and institutions: Living in a material world. ***Theory and Society***, 37(5): 461-483.

companies and governments among many others) may be obstacles to organizing information flow differently. This is confirmed by how MAW, which operated in a more open and unconventional manner than SGG, found it more difficult to get acceptance and legitimation. Instead, SGG managed to cement an alliance with media to challenge governments so creating a short circuit between the two, which was skilfully framed by a patriotic and democratic narrative (here I am not investigating if it was the true motive or not, but only that it was consistent and convincing throughout[22]).

The two contrastive cases question also the overemphasis on openness that many internet circles put at the center of their practices and aspirations (Miscione, Pfeffer, Martinez, & De', 2013). Provocatively, one may say that assuming that data is everything is like thinking that Hollywood is just about arranging pixels on our screens. Technically it is the case, but data – it does not matter how big – become part of organizing processes as information and narratives. So, updating Benjamin, narratives are to data as constellations are to stars: you see some, you grasp the rest. In case this sounds too contemplative for business research, it is poignant to stress that media framing of leaked data by means of legitimized narratives allowed an overflow of issues like privacy and accountability in the contemporary global context into the international political arena. On the other hand, lack of easily recognizable narratives produced confusion and several dead-ends for MAW. In other words, narratives as organizing principles of data facilitated allocation of responsibility, thus performativity.

On their side, by maintaining its traditional role of story-telling by selecting, framing and curating, SGG journalists demonstrated a healthy distance from the organizations they are expected to watchdog.

Dramas of Institutional Identification

In summary, we have two cases both dealing with large amounts of confidential data. MAW operates according to the practices and social models (i.e. institutions) that originated and developed (on) the internet, well synthetized by the motto "we reject kings, presidents and voting. We believe in rough consensus and running code" (David

[22] These emplotted personal and patriotic narratives have been iterated in the interview to the US television NBC on May 28th 2014.

Clark). They clashed with society at large. SGG has conceded a central role to journalism, which has mediated between the online praxes and broader contemporary society. So, SGG demonstrated a sometimes tense but overall successful process of identification with fundamental institutions of Western societies. This institutional identification granted SGG a remarkable resonance and acceptance, therefore performativity on the public sphere.

The differences do not mean that MAW and SGG disagreed in principle. Their principles of democratic transparency and accountability are quite similar. The way those principles get engendered and accepted by societies mismatches. So, claiming truth vs. falsehood seems simplistic to frame the two cases. All protagonists justify their actions as motivated by unveiling the truth. However, there is a difference about how they portray their antagonists: SGG reveals the secret that US government holds and claims to be patriotic by appealing to a foundational freedom principle of America. MAW maintains that all governments lie. This opposition recalls Greimas's semiotic square.

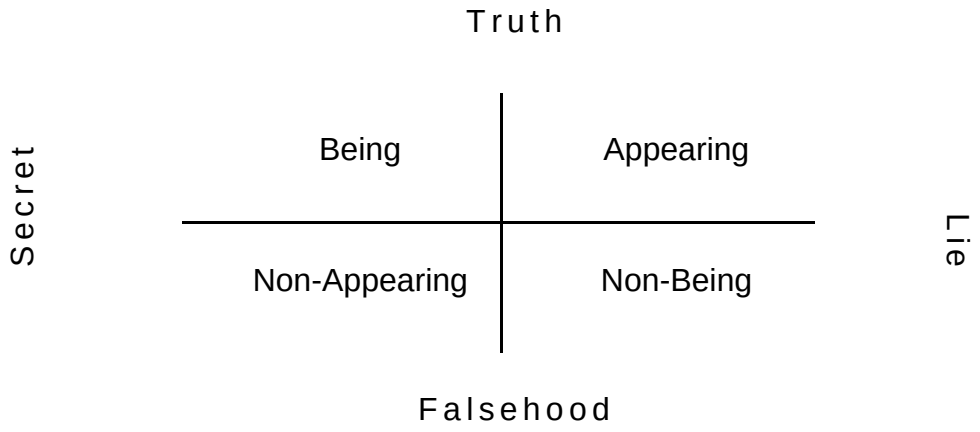

Table 1: adaptation of Greimas' semiotic square

As states have always been allowed to have secrets, SGG portraying its antagonists as holding secrets unduly allows it to maintain a level of legitimacy that is denied to MAW, whose stance is clearly expressed in recent Assange, Appelbaum, Müller-Maguhn, and Zimmerman (2012) book along the lines of crypto-anarchism summarized by the maxim "privacy for the weak and transparency for the powerful". So, Greimas's

square can help positioning different dramatization strategies in relations to established institutions.

New real politik: data realism vs. communication realism

"Like composers, we cannot write music for which there is no instrument" (Howard Becker). Another difference is worth a deeper discussion. Both MAW and SGG aim at showing the "reality out there" that people are not aware of. So, realism is not intended here in the sense of empiricism or positivism but in the sense of real politik, of pragmatic understanding of how things work and acting accordingly. This may seem obvious but several actors showed no understanding of the reality they were dealing with. For instance, in both MAW and SGG cases high officials suggested that clemency could be considered if all copied files were deleted. This means seeing a file chase like a car chase in a Hollywood movie. Instead, once files – encrypted or not – are out there, there is no possible way to restore a previous order. Implying the opposite undermines irreversibly the credibility of the speaker as if s/he believed that actors shot in films die for real. On the other side, those cases are a sort of reality checks for some technological utopias: those leaks showed the failure of cryptography grand vision of allowing stealth actions on the global scale; problems with a security protocol called OpenSSL and the encryption software TrueCrypt tainted free and open source as an organizational model with doubts. These are examples of how the world converges with what are usually perceived as mere (technologies of) representations[23]. Realizing the scope of what is possible and what is not is basic for any intentional action in any context.

Without digressing into what is real, I simply adopt a quite minimalistic definition of what it means here: reality is what cannot be changed at will (Eco, 1994; Ferraris, 1999)[24]. This means, in Social Construction of Technology terms, to debate the concept of interpretative flexibility (Pinch & Bijker, 1987) by identifying its boundaries.

[23] See also Czarniawska, B. 2013b. Things and Words. ***Journal of Change Management***, 13(3): 362-367.
[24] A sort of genealogy of realism in novels and social sciences can be found in chapter 4 of Czarniawska, B. 1999. ***Writing management: Organization theory as a literary genre***: Oxford University Press, USA.

Both MAW and SGG act in the name of realism, but in remarkably different ways. MAW manifests realism by minimizing its story-teller/curator role (as it would inevitably mean “sanitizing” data) and expecting that data would speak by themselves. This can be called data realism. SGG is realist by acknowledging the rules of the communication game and using narratives strategically. Therefore it can be labelled communication realism. A raw semiotic of action nets can explain MAW and SGG: data and actions make sense (or not) according to a (lack of a) narrative, therefore coherent outcomes manifest and actor-networks may stabilize. But there is probably something else beside narratives as sense-making devices for organizing data, technologies and actions.

There was a climax in science fiction and common sense about the illusions that electronic communication creates in societies vs. real, hard facts. This probably culminated in the popular narrative of the trilogy Matrix. Those terms are inverted in the cases presented here. Real, well-established organizations like Western states and governments flew the flag of open communication, especially against countries like China, while they have been using those same infrastructures for an unprecedented intelligence surveillance. On the other hand, people inhabiting information networks showed what was happening behind closed doors. So, here reality and fiction seems to have swapped side: states fictionalize, electronic communication brings reality back in.

I would like to suggest that, after having followed the action (as Czarniawska emending Latour would recommend) for quite some time, we should become more knowledgeable about this new context of action that information infrastructures contribute to generating. On the basis of the above, it is possible to suggest that the traditional hierarchy of concepts of information studies (data – information – knowledge – wisdom) can be developed into the following: data – information – plots – legitimacy. In fact, following the comparison of MAW and SGG, one can see that the framing and emplotting operated by media facilitated the overflow of the whistleblowers’ message into the political arena. Therefore media as institutions enhanced the legitimacy and then performativity of whistle-blowers.

As a final remark, I would like to stress that one can see no signs of the emergence of an ideal speech situation or of some sort of idealized agora. Rather, global information

infrastructures move clearly in the direction of becoming a 'world wild west', i.e. an arena for confrontation where no rule seems to hold. This goes far beyond the main players and affects everyone, for example now the simple doubt that communications are intercepted and scrutinized may undermine anyone intending to engage in sensitive issues online, or even to have the necessary private space where to develop autonomously own stances (Introna, 1997). Paradoxically, one might even say that not knowing about NSA could have been less detrimental. In any case, data are irreversible, we cannot go back to the silence that large organizations simulated.

Acknowledgements.

I would like to thank Daniela Landert for our conversations on this topic and for her comments, Mary Canning and Donncha Kavanagh for their generous attention and helpful suggestions.

REFERENCES

Anderson, C. W. 2010. From Indymedia to Wikileaks: What a decade of hacking journalistic culture says about the future of news, ***Nieman Journalism Lab***: Nieman Foundation at Harvard.

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmerman, J. 2012. Cypherpunks: Freedom and the future of the internet: New York: OR Books.

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. 2012. ***Cypherpunks: Freedom and the Future of the Internet***: Or Books.

Benkler, Y. 2006. ***The wealth of networks: How social production transforms markets and freedom***: Yale Univ Pr.

Benkler, Y. 2012. A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate. ***Harvard Civil Rights-Civil Liberties Law Review***, 47(1).

Benkler, Y. 2013. WikiLeaks and the networked fourth estate. ***Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society***: 11.

Berners-Lee, T. 1989. Information management: A proposal.

Boczkowski, P. J. 2009. Technology, monitoring, and imitation in contemporary news work. ***Communication, Culture & Critique***, 2(1): 39-59.

Boczkowski, P. J., & Mitchelstein, E. 2013. ***The news gap: When the information preferences of the media and the public diverge***: MIT Press.

Bowker, G. 2000. Biodiversity Datadiversity. ***Social Studies of Science***, 30(5): 643-683.

Bowker, G. C., & Star, S. L. 1999. ***Sorting things out: classification and its consequences***. Cambridge, Mass. [u.a.]: MIT Press.

Bruns, A. 2012. Reconciling community and commerce? Collaboration between produsage communities and commercial operators. ***Information, Communication & Society***, 15(6): 815-835.
Coleman, E. G., & Golub, A. 2008. Hacker practice Moral genres and the cultural articulation of liberalism. ***Anthropological Theory***, 8(3): 255-277.
Coleman, G. 2004. The political agnosticism of free and open source software and the inadvertent politics of contrast. ***Anthropological Quarterly***, 77(3): 507-519.
Coleman, G. 2011. Hacker politics and publics. ***Public Culture***, 23(3 65): 511-516.
Conboy, M. 2004. ***Journalism: a critical history***: Sage.
Corvellec, H., & Czarniawska, B. 2014. For more sustainable cities: action nets for waste prevention, ***EGOS***. Rotterdam.
Czarniawska, B. 1999. ***Writing management: Organization theory as a literary genre***: Oxford University Press, USA.
Czarniawska, B. 2008. ***A theory of organising***. Cheltenham: Edward Elgar Publishing.
Czarniawska, B. 2011. Performativity in place of responsibility? ***Journal of Organizational Change Management***, 24(6): 823-829.
Czarniawska, B. 2012. ***Cyberfactories: How news agencies produce news***: Edward Elgar Pub.
Czarniawska, B. 2013a. On meshworks and other complications of portraying contemporary organizing, ***GRI-rapport***, Vol. 3. Gothenburg: Gothenburg Research Institute.
Czarniawska, B. 2013b. Things and Words. ***Journal of Change Management***, 13(3): 362-367.
DeNardis, L. 2012. Hidden levers of Internet control: An infrastructure-based theory of Internet governance. ***Information, Communication & Society***, 15(5): 720-738.
Dutton, W. H. 2009. The fifth estate emerging through the network of networks. ***Prometheus***, 27(1): 1-15.
Eco, U. 1994. ***The limits of interpretation***: Indiana University Press.
Ferraris, M. 1999. La fenomenologia e il Messia. ***Aut aut*** 293-294: 167-182.
Floridi, L. 2012. Distributed Morality in an Information Society. ***Science and engineering ethics***: 1-17.
Goody, J. 1986. ***The logic of writing and the organization of society***: Cambridge University Press.
Greenwald, G. 2014. ***No place to hide - Edward Snowden, the NSA, and the U.S. Surveillance State***: Metropolitan Books.
Habermas, J. 1989. ***The theory of communicative action: Lifeworld and system: A critique of functionalist reason***: Beacon press.
Hintz, A. 2013. Dimensions of Modern Freedom of Expression: WikiLeaks, Policy Hacking, and Digital Freedoms. ***Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society***: 146.
Introna, L. D. 1997. Privacy and the computer: why we need privacy in the information society. ***Metaphilosophy***, 28(3): 259-275.
Kerckhove, D. d. 1997. ***Connected intelligence: The arrival of the web society***: Somerville House, USA.
Knorr-Cetina, K., Schatzki, T. R., & Von Savigny, E. 2000. ***The practice turn in contemporary theory***: Routledge.
Landert, D. 2014. ***Personalisation in Mass Media Communication: British online news between public and private***: John Benjamins Publishing Company.
Latour, B. 2005. Reassembling the Social: an Introduction to Actor-Network-Theory. ***Oxford, Oxford University Press***, 16: 207.

Lewis, S. C. 2012. The tension between professional control and open participation: Journalism and its boundaries. ***Information, Communication & Society***, 15(6): 836-866.

Manovich, L. 1999. Database as symbolic form. ***Convergence: The International Journal of Research into New Media Technologies***, 5(2): 80-99.

McLuhan, M. 1962. ***The Gutenberg galaxy: the making of typographic man***. London: Routledge & Kegan Paul.

Miscione, G. 2000. hAcK3rZ and Information Warfare. ***Quaderni di Sociologia***: 22-47.

Miscione, G. 2011. Global Visibility and Local Accountability - Making Sense Out of (Human) Sensors, ***ICT4D – The Development Impact of Information and Communication Technologies***. Switwzerland: ETH Zurich.

Miscione, G., Pfeffer, K., Martinez, J., & De', R. 2013. Openness may not Mean Democratization - e-Grievance Systems in their Consequences, ***N-AERUS***. Enschede: University of Twente.

Newman, N., Dutton, W. H., & Blank, G. 2012. Social Media in the Changing Ecology of News: The Fourth and Fifth Estates in Britain. ***International Journal of Internet Science***, 7(1): 6-22.

Nicolini, D. 2009. Zooming In and Out: Studying Practices by Switching Theoretical Lenses and Trailing Connections. ***Organization Studies***, 30(12): 1391.

Nicolini, D. 2012. ***Practice Theory, Work and Organization. An Introduction***: Oxford university press.

North, D. C. 1990. Institutions, institutional change and performance. ***Cambridge: CUP***.

Ong, W. J. 1982. ***Orality and literacy: the technologizing of the word***. London: Routledge.

Ostertag, S. F., & Tuchman, G. 2012. When innovation meets legacy: citizen journalists, ink reporters and television news. ***Information, Communication & Society***, 15(6): 909-931.

Pinch, T. 2008. Technology and institutions: Living in a material world. ***Theory and Society***, 37(5): 461-483.

Pinch, T. 2009. On making infrastructure visible: putting the non-humans to rights. ***Cambridge Journal of Economics***, 34(1): 77-89.

Pinch, T. 2010. The invisible technologies of Goffman's sociology from the merry-go-round to the internet. ***Technology and Culture***, 51(2): 409-424.

Pinch, T. J., & Bijker, W. E. 1987. The Social Construction of Facts and Artifacts: Or How the Sociology of. ***The social construction of technological systems: New directions in the sociology and history of technology***, 17.

Poster, M. 1997. Cyberdemocracy: Internet and the public sphere. ***Internet culture***: 201-218.

Powell, W. W. 1990. NEITHER MARKET NOR HIERARCHY. ***Research in Organizational Behavior***, 12: 295-336.

Powell, W. W., & DiMaggio, P. J. (Eds.). 1991. ***The New Institutionalism in Organizational Analysis***. Chicago, London: The University of Chicago Press.

Surowiecki, J. 2005. ***The wisdom of crowds***: Random House Digital, Inc.

Verplanke, J., Martinez, J., Miscione, G., Georgiadou, Y., Coleman, D., & Hassan, A. 2010. Citizen Surveillance of the State: A Mirror for eGovernment? In J. Berleur, M.D. Hercheui, & L. M. Hilty. (Eds.), ***What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience***: 185-201. Berlin: Springerlink.

Weick, K. E. 1993. The collapse of sensemaking in organizations: The Mann Gulch disaster. ***Administrative science quarterly***: 628-652.